

Public key infrastructure

Publication number: EP1117207

Publication date: 2001-07-18

Inventor: CORELLA FRANCISCO (US)

Applicant: HEWLETT PACKARD CO (US)

Classification:

- international: **G09C1/00; H04L9/32; G09C1/00; H04L9/32; (IPC1-7): H04L9/32**

- european: **H04L9/32T**

Application number: EP20010300224 20010111

Priority number(s): US20000483356 20000114

Also published as:

US6763459 (B1)
JP2001249612 (A)
EP1117207 (A3)
EP1117207 (B1)
DE60105326T (T2)

Cited documents:

WO9935783
US5982898
WO9919845
XP002173298
XP000997964

Report a data error here

Abstract of EP1117207

A PKI (30) includes an off-line registration authority (38) that issues a first unsigned certificate (60) to a subject (34) that binds a public key (62) of the subject to long-term identification information (63) related to the subject and maintains a certificate database (40) of unsigned certificates in which it stores the first unsigned certificate. An on-line credentials server (42) issues a short-term disposable certificate (70) to the subject that binds the public key of the subject from the first unsigned certificate to the long-term identification information related to the subject from the first unsigned certificate. The credentials server maintains a table (44) that contains entries corresponding to valid unsigned certificates stored in the certificate database. The subject presents the short-term disposable certificate to a verifier (36) for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key (46) in the short-term disposable certificate.

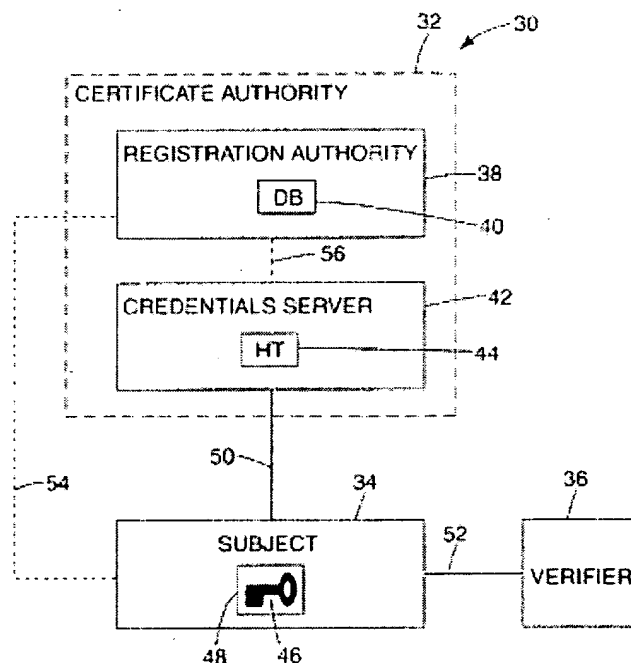


Fig. 1

Data supplied from the **esp@cenet** database - Worldwide